International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-10 Issue-1, October 2020

Information Security Risk Analysis Methods for Healthcare Systems

Amarendar Rao Thangeda, Alfred Coleman

Abstract: ***Information and risk analysis in healthcare system is an important issue in the modern technological growth. There are many systems implemented for information security and risk management for information protection. Proper guidance is needed to select the system as all the systems concentrate on information security of healthcare system. The information threats and risk are increasing, and all the issues are integrated to the vulnerabilities producing risk for the healthcare security. The healthcare system process structure and variation are advocated, in which operating performance indication is based on risk scaling factor so that dynamic information security risk analysis is needed. This paper is proposed for information security risk analysis in which the resources, risk threats, vulnerabilities that control the healthcare system. The paper compares the various inputs and outputs are needed by different systems of information security risk assessment and analysis that accurately presents the information security risk. At present, large number of information security risk analysis methodologies are present in the worldwide. Important and efficient methodologies are considered for comparison and quantitative purpose to choose most suitable methodology for healthcare system.***

Keywords: Information security risk analysis, healthcare security system, risk assessment, risk threats, risk vulnerabilities

I. INTRODUCTION

The information security risk analysis is used to protect the information with various methods to reduce the risk and threats. The healthcare systems are highly investing on information security to reduce the risk and to secure the information resources to avoid information loss due to risk threats. The encryption of information data is the one of the most popular information security measure. The encrypted information may be intruded by the instruction hackers due to less protection provided by the methodology. Therefore, various methodologies are emerging towards information security in healthcare domain to protect the information about the patient and hospital management information [1]. The information security system research has becoming a major research and development in various departments such as healthcare. The researchers have incorporated various theories and methodologies references from various disciplines. The existing status of security and risk management in healthcare, incorporating numerous research methodologies to solve risk problems such as research and development of information security, qualitative and quantitative information security system with risk assessment, comparison on various methodologies. The healthcare institute wanted to maintain the confidential information with accountability and authentication should be given to the users those have the proper hierarchy permission. This article forwards the framework for selecting the easy method for information security management using various information security approaches. There a huge number of risk analyses were implemented, and major objective is to suggest which task to be used for higher security [2].

Revised Manuscript Received on September 25, 2020.

* Correspondence Author
Amarendar Rao Thangeda*, Faculty of Computing, Botho University, Gaborone, Botswana, E-mail: amarendar.thangeda@bothouniversity.ac.bw
Prof. Alfred Coleman, Computer Science Department, University of South Africa, Pretoria, South Africa, E-mail: colema@unisa.ac.za

II. INFORMATION SECURITY IN HEALTHCARE SYSTEM

The information security in healthcare based on centralization protection for high security to reduce the risk factors. Every authorization is given based on digital audition only. The secured metrics are also given for each person to enter the secured area to get the authentication through the centralized distribution of the authority.

III. INFORMATION SECURITY RISK IMPROVEMENT

Reference [2] have presented the information security system based on OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) methodology.
The various problems like assets, vulnerability process, and dangerous threats are operationally solved by OCTAVE procedure. OCTAVE is the technique proposed for information security risk management to evaluate information security risk in an organization. It is helped in different ways to an organization are,

1) Asset monitoring
2) Quantitative security risk analysis for risk tolerance criteria
3) Finding vulnerabilities on assets
4) Finding information threats
5) The realized threats should be evaluated with potential technique

The OCTAVE method was established at Carnegie Mellon University in 1999. The inventor of OCTAVE is Software Engineering Institute (SEI).

The high-level language was used to perform OCTAVE for security risk analysis and giving the solution to protect the organization information.

Table 1: OCTAVE and version update of timeline

Date	Publication
Sep 1999	Ver 1.0 of OCTAVE Framework
Sep 2001	Ver 2.0 of OCTAVE Framework
Dec 2001	Ver 2.0 of OCTAVE Criteria
Sep 2003	Ver 0.9 of OCTAVE - S
Mar 2005	Ver 1.0 of OCTAVE - S
Jun 2007	Ver 1.0 of OCTAVE Allegro

The Table 1 shows that the octave and its version update of timeline. The upgraded version is introduced by OCTAVE team with high performance for security risk management.

With high efficiency of OCTAVE method is invented for information security risk management with different versions were introduced. In the technical documentation of OCTAVE mentioned that three different OCTAVE methods are published for organization usage. They are classified as OCTAVE method, OCTAVE - S method and OCTAVE Allegro method are the classification types. Each of above mention OCTAVE methods has unique features to protect the information with streamline methodologies to protect the asset of information. The OCTAVE improved versions have move features such as accountability, auditing and user friendly for the authorized section of the organization.

The OCTAVE methodology is implemented in 3 phases. In phase 1, the security risk analysis technical team defines the significant information of assets and the security strategy of assets is suggested. The security risk analysis technical team finds the assets which is most priority to the organization activities, reports to the information security requirements, and finds information threats that will interrupt the other requirements of the assets. In phase 2, security risk analysis technical team makes the evaluation criteria on information system to provide the information threat analysis done in the phase 1 and to intimate decision making for next phase. In phase 3, security risk analysis technical team does information security risk identification significant activities and produces the risk management plan to protect the information of the organization.

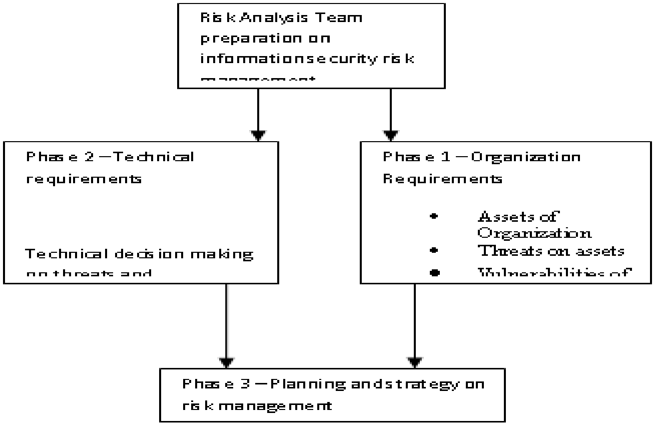
Risk Analysis Team preparation on information security risk
Phase 2 – Technical requirements
Technical decision making
Phase 1 – Organization Requirements
Assets of Organization
Threats on assets
Phase 3 – Planning and strategy on risk management

Figure 1: Phases of OCTAVE method

The figure 2 shows the 3 phases of OCTAVE methods for organization information security management. The development of OCTAVE methodology leads to next level called OCTAVE - S methodology that have similar 3 different phases. The OCTAVE - S also executed by the security risk analysis technical team to process the security system. But OCTAVE - S security risk analysis technical team may not have formal prior knowledge to convey information since it is guessing that the security risk analysis technical team has analytical capability on the task-based information security management system with practical application of the organization. The OCTAVE Allegro methodology is applied to the organization for information security to reach the goal of high protection on asset and eliminate the threats and vulnerabilities. It is robust and without the requirement for extensive risk management knowledge for the security risk analysis technical team. The methodology is user friendly and those who have the authority, the proper report and guidance are given by the OCTAVE Allegro methodology to handle the information security risk analysis. The OCTAVE Allegro methodology is entirely different from OCTAVE - S methodology including the storage and transport of data and processing system. The handling the vulnerability and threats are very efficient and information security is highly efficient. This methodology is working on the collaborative setting and workshop manner and it is highly support with guidance and worksheet, question answer manner, and all information about handling the process is given in the appendices of the report. The OCTAVE Allegro is highly applicable for the usage of individuals those want to implement the information security risk assessment without high executive movement and expert advice or input and output.

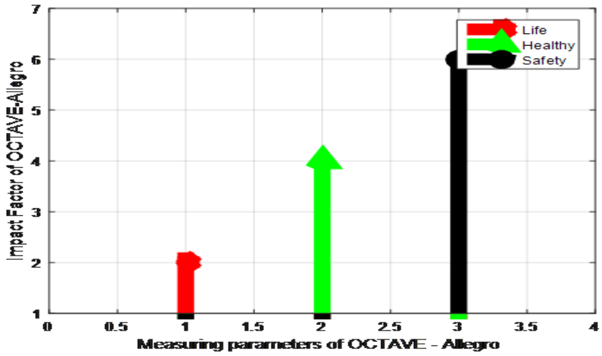

Figure 2: Measuring parameters of OCTAVE-Allegro

The figure 2 show that the measuring parameters of OCTAVE-Allegro with respect to its impact factor. By using OCTAVE-Allegro methodology, the customers or patients lives are even threatened; they will be recovered after the proper medical treatment. Its impact factor is moderate. There is no harm or particular risk to patients in lives. The impact factor is low. OCTAVE-Allegro gives high priority to reputation and customer confidence, financial, productivity, safety and health, fines and legal activities, and user defined also initiated. Reference [3] has presented a relative framework for evaluating Information Security Risk Management methods. The organizations and other sectors including healthcare are highly affected by the government and industrial policies of risk management systems. Many policies are available to control, identify, measure the events of information risk management. The authors have constructed the planning based on CobiT to control the organization assets risk and vulnerabilities. The CobiT is used for declaring of particular audits and outcomes including government institutions and other private sectors like healthcare department. It is an international best practicing methodology including bridging the forbidden gap between economical risk and technical problems needed to be control. It provides different kinds of risk management and risk are grouped as regular, technical and continuous manner. The defined risk tolerance profile of organization is suggested in the framework that will agree a particular level of information security risk that is indicated by the risk tolerance procedure. Then the risk action plan will be executed by the organization committee to solve the risk security issues on information. It is a cost-effective manner to protect the information of the healthcare and other organizations. The risk management is executed irrespective of industrial level and it follows the particular risk assessment steps. Different risk assessment methodologies have various procedures that change in different objectives. The planning and execution of policy is considered the plan, do, check and correct (PDCC) those are indicated in CobiT. Based on these phases the generic risk assessment policy is generated to identify, measure, monitor, and control the risk. Reference [4] has presented existing status of research in information security and privacy in the healthcare sector. The technological growth in healthcare section, all documentation is digitized and stored in the cloud or other storage devices. The information exchange between patients should be avoided and information should be protected in a high accurate and efficient manner. The information security and privacy in healthcare including patient’s health information, legal information and notification, medicines, the industrial reports are important and should be protected using information security management system. The risk factors are generated from different threats and outside hackers to the healthcare sector information to hack the information about the patients and hospital. The healthcare threats can be grouped into four different classes; motives, resources, accessibilities and capability of technology. Based on these categories, various threats and risk may give different level of information risk to the healthcare to plan the prevention methodology. The intruder motive may be economic threat or non-economic threat. The healthcare sector is highly responsible for intruder threats. There is some intruder may steal the information to fulfill the economic value by selling the information to other organizations. Some intruders may steal the information to blackmail the patients regarding to raise some political or social problems. The healthcare sector information is recently in use of information in various formats. The distribution of information inside the healthcare section is the major problem and there is a chance of stealing the information while distributing among other departments. The technological growth in internet has very good business model and development for online business industries and financial services. The online service is introduced to healthcare section such as health monitoring, online consulting with doctor, e-billing, e-services of patients are established for patient information transformation from one place to another through the internet. The e-services of information should be secured through online and protect the patient information and eliminate the risk factor. The information managing and security risk management is a difficult execution and it needs large investment to healthcare resources and highly efficient and accurate approach is needed. OCTAVE approach is the appreciable approach for protecting the healthcare information based on asset security for information security assessment. Reference [5] has presented different information security risks to make the framework between different methodologies for Information Risk Management. The various quantitative and qualitative methodologies were analyzed in terms of performance. The qualitative methods are classified as OCTAVE and CORAS (Construct a platform for Risk Analysis of Security Critical Systems). The CORAS method was proposed by Stolen et al. in the year of 2002. The qualitative methodologies are classified as first one is ISRAM (Information Security Risk Analysis Method) introduced by Karabacak and Sogukpinar in the year of 2005. The second one is Cost-Of-Risk Analysis (CORA) method was introduced by International Security Technology Inc (IST Inc) in the year of 2000. The third one is Information Systems (IS) analysis based on a business model Suh and Han *et al.* in the year of 2003. CORAS was developed under the Information Society Technologies (IST) program by Stolen et al. in the year of 2002. The CORAS was implemented by the Information Society Technologies (IST) for Information Security Risk Management application. The major functionality of CORAS is to for the useful procedure for information security risk analysis, the semi-procedure method for object-oriented methodology and software tool for an accurate, very clear, and efficient assessment for Information Security Risk Management. This is very useful methodology for healthcare and other organizations for providing the security for information threats using CORAS profile. The communication efficiency also high and therefore the UML profile is proposed by CORAS have applied to reach the high-quality information security risk analysis. The ISRAM methodology for information security risk analysis was implemented during the year of 2003 at the National Research Institute of Electronics and Cryptology and Gebze Institute of Technology in Turkey. The proposed methodology is an important quantitative process to information security risk analysis that provides significant of the different levels of healthcare sector and other organization manager and other staff based on the authority hierarchy. The probability and consequence are two different and autonomous surveys are established for the information security risk management.

The ISRAM does not utilize the methodology such as Single Occurrence Losses (SOL) or Annual Loss Expectancy (ALE); the risk factor also estimated in-between 1 and 25. The estimated numerical analysis is directly related to qualitative, high, medium or less value for information security risk management analysis. The IS risk management is related to Business Model was established at Korea Advanced Institute of Science and Technology in the year of 2002. This methodology was proposed to overcome the limitations of existing methodologies for information security risk analysis. The IS analysis is used for reducing the running cost for providing the security for information during the risk analysis and management for an organization and healthcare section. The methodology is proposed as four different stages. Some of the common objectives were founding during the analysis of above-mentioned methodologies, such as,

- The information security risk analysis is conducted on single or group of assets
- The major algorithm used
- The management staff involvement in information security risk analysis
- The risk analysis results are efficient and accurate based on testing procedure for information security

Reference [6] has presented risk management framework for information security risk analysis. The security risk is generally described as the risk list, grouped in the proper order with highly risk factor first and other or grouped based on the priority of risk factor. The risk management system is established for an organization to provide the information security. The risk management structure is organized based on the risk criteria. The organization risk management is mainly used to identify the risk, estimate the assets, assess the security control and give the proper communication to the appropriate authority about the information risk handling. The organization authority committee will implement the risk control to modify and provide the risk handling in efficient and accurately.

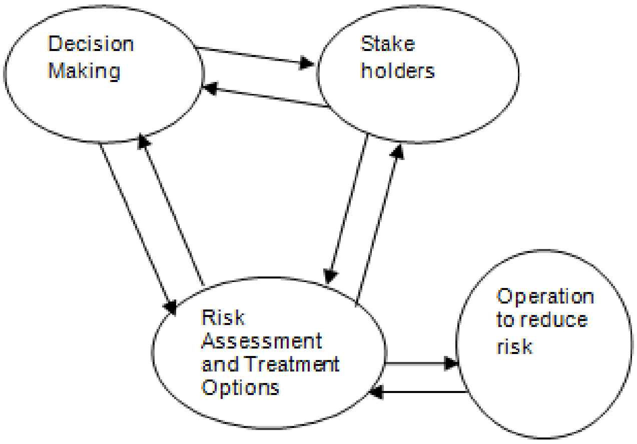

Figure 3: NERAM Risk management benchmark

The figure 3 shows that the basic functionalities of risk management system and the linkages are related to higher range of risk management framework for information security. This is the conventional risk management system implemented over last decades with conventional technology. It is based on the three different models such as risk estimation, risk evaluation and risk treatment options.

Reference [7] are presented the risk management for healthcare organization based on an enterprise model. The Committee of Sponsoring Organization of the Treadway Commission (COSO) has released a summary on Enterprise Risk Management (ERM). The title of publication is “Enterprise Risk Management – Integrated Framework”. The summary suggests the information security risk management team such that ERM effective process can be made by the organization of healthcare section team and board of directors can respond to the suggestions made by the team. The internal or external risk management control execution can be done based on the priority of risk analysis.

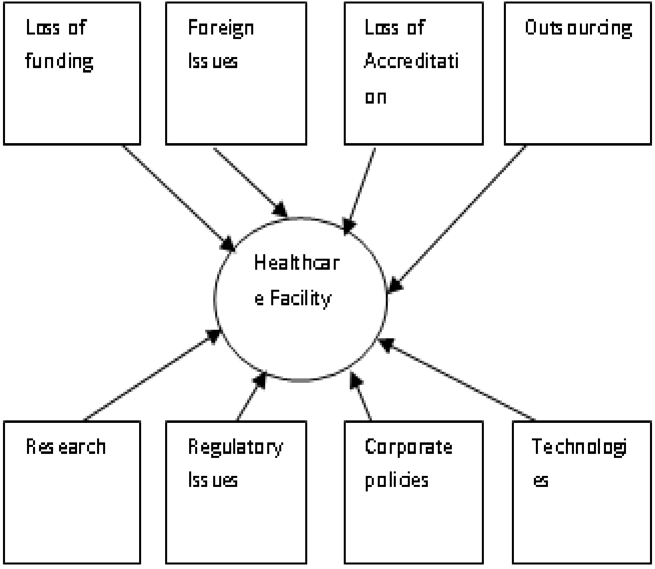

Figure 4: Healthcare sector problem finding

The figure 4 illustrates the problem finding of the healthcare sector. The ERM achievement is effective made by analysis of the problems faced by the healthcare industry. The all the problems are listed out by the risk management team. The operational, financial, human, strategies, legal/regulatory and technologies risk factors are associated in the problem finding for risk analysis. In today’s healthcare section, the embracement achievement is achieved based on ERM for incorporating the problems and provide the accurate and efficient solution for information security risk analysis.

Reference [8] are presented the information management system for privacy and security in health information risk assessment and management. The healthcare sector has captured and stored the information in digital format. The patient information is very personnel and secrets that should be stored in databases keep in private and security. The confidentiality, integrity and availability of information should be confirmed on healthcare sector. The conventional methods of measuring asset are in terms of dollars. The method is very difficult, and the measurement of asset may change intangible assets to dollars. The assets are calculated as information database to main the information security risk factor.

The technological issues are rectified by applying the technique methodologies using business policies, management principles and training of the healthcare section staff and providing the awareness them. The technological solution is provided based on the business network, authorization, authentication, auditing and encryption the information from the database. The healthcare section staff behavior also considered for security purpose. The identification of well-known practice and unknown practice should be taken into account for information risk management ERP preparation based on the technology. The ERP construct the scenarios about the information threats to information assets. The sufficient database is generated using ERP model to examine the security of information. The threats identification is the extracting the significant information from the information database. The threats have to be eliminated technologically using ERP model based on the historical assignments made by the healthcare sector authority people. The estimation of assets values has to be maintained throughout the healthcare sector establishment and running without losing the information security by the ERP technological solution for ERP management. The information evaluation should be made in efficient and accurate methodology using ERP management to secure the information assets based on the encryption technology. The information vulnerability threats have to be reduced and eliminated using ERP model by providing the technological solution. Reference [9] is presented risk management system for healthcare section based on its information structure and workflow to provide the information security for the patients and hospital database information. The patient database in the hospital is stored to take care of patients. It has high potential in incorporating the data with genetic database information from patient to give proper decision making for diagnosis and therapy decisions. The data mining technology is used in the healthcare sector for storing the data for storage and other activities such as technical, economical and legal decision making. The healthcare clinical support methodology is higher catalyst for doing evidence-based medication in healthcare sector. The patient database is incorporated with Electronic Patient Records (EPR) as information source for data mining technology for information security to reduce the risk factors. The rules of association can be established for data mining development. The logical implementation of system is possible to issue the explanation about the information generated by the healthcare organization persons with confident and efficient. There is high potential of information security system to increase the quality and accuracy of hospital database maintenance based on the workflow and information integration. Healthcare sector workflow indicates the human resources such as doctors, nurse, housekeeping staff and patients and they can help to improve the standardization of information security process based on the workflow simulation and implementation process. The data collection is tabulated as short format for data mining to secure the information. The database storage is based on XML database maintenance policy. The syntax specification is used to enable accurate web service since web-based storage such as cloud can be development for data mining process. It is used for both algebraic and analytical process to store the information security to reduce the risk and threats. Reference [10] is presented risk management framework for information security risk analysis and compliance-based solution to reduce the risk and threats on information maintenance. The risk management enterprise is established to process the effective entity group of organization of healthcare sector. The board of directors, organization higher authority, doctors, enterprise persons, nurses and other authority staff are grouped as one entity and they manage the risk factor with risk appetite to issues the reliable assurance for information security to achieve the objective. The information security and compliance-based solution will give the balanced solution on information database maintenance and secure the data to protect from hackers. Reference [11] has presented the solution for healthcare sector to manage the information safety risks. In the healthcare sector, the management committee is organized by the higher authority and effective risk management is processed by the committee. The involvement and cooperation of management committee is required for risk management assessment. The working ability of the team has to satisfy the committee on the risk management to solve various problems related to patients, doctors and other staff to solve the problems technically and reduce the external press of the human resources. To finalize the committee of the management the following criteria are needed,

- Health and safety issues involvement
- The health and safety assurance investment of time and money
- Responsibilities are highly understood to ensure health and safety

The workplace of healthcare sector should be safe and healthy and clear notification is needed about what could wrong in the workplace and what should be repeated. The risk management committee should search and find out the hazard cause from various sources. The risk management committee should understand the source of harm properly and the reason of harm occurrence and what are all the effects will be caused due to the presence of hazard, everything should be listed. To control the harm caused by various sources should be proceeded by the risk management committee. The management committee should involve on the consultation of information with the workers to generate the reasonable chance to express the opinion on the cause and the decision making should be generated based on the consultation and conversation. The required safety matters and measure should be consulted with the healthcare section staff and should be provided to management the risk factors. Reference [12] has presented information security risk management system and the security solution for the investing for risk management and assessment. Due to increase in various organization and industries including healthcare section, the information security threats, and wrong decision making may cause the risk management critical and dangerous. The security should be provided through risk assessment, risk evaluation, etc., the technique is suggested by the authors to provide the risk management for proper investment efficient manner.

Step 1: Detail analysis is required for getting investment from the healthcare section
Step 2: Give the proof for investment efficiency
Step 3: Should not depend on the IT security sector for human safety

The various developments made to improve the Information Security Risk Management (ISRM) community to give proper support to risk management team to provide efficiency and accurate security decision making, and that should be healthcare mission should be given to the patients as well as staff members. The ISRM methodology is useful in business process to improve the economical level of the healthcare sector by providing the information risk assessment and management. It automatically estimates the significance of assets that are needed by the different activities of the process. Reference [13] have presented the risk management system based on risk assessment framework and important techniques suggestion for proper and efficient risk management to the organization. The author highly concentrates on safety transportation of harmful and dangerous goods from one place to another of Dangerous Goods in the Baltic Sea Region (DaGoB). The improvement of cooperation and integration at different levels of administration and patients of management hierarchy is important to ensure the safe and efficient risk management system good. The packing the dangerous goods are also very harmful sometimes, the safety measure should be considered for reducing the risk factors.

Reference [14] provides the risk management system for an organization is based on the International Standardization Organization (ISO) 3000 certificate. The methodology is provided to risk management to keep the high potential impact on the different risk processes activities, various products and services. The successful approach will give the organization profit and many other beneficial such as economical and legally not affected the organization. The risk may affect the organization in different terms such as short, medium and long. These risks should be managed by providing proper operations handling by the appropriate team with intelligent tactics and strategies. The strategy plan may be kept by the organization for more than 5 years. If any necessary changes are needed, that can be processed by the proper channel through the authority of the organization. The scope of risk, nature of risk and risk evaluation are listed in the documentation and that should be properly monitored by the authority team to make the risk tolerance and appetite and attitude. The risk response should be carried out by the proper treatment process and risk should be controlled. The potential factor to control the risk should be successfully implemented in an organization. The risk management is centralized portion of an organization management. The activities of the organized should be well defined to reduce the risk factor. The activities should be carefully handled by the appropriate person or team carefully to avoid risk factor to improve the risk management ability.

Reference [15] have presented the methodology for security risk management to improve the information security efficiency and accuracy. The enterprise should satisfy the government and industrial safety requirement to reduce the risk factor to optimize the risk to information protection. The risk management assessments and analysis are difficult process that should generate data that issue organization decision making on safety and risk factor optimization. The COBIT (Control Objectives for IT and Available Technology) gives the entire control setup that can be carried out to conduct the test for risk assessment for information risk management based on information technology. The critical risk assessment should be properly determined on the organization lower level and higher level of hierarchy to maintain risk factor level low. The testing the quality of service at every phase of work at organization should be made efficient and accurate. The customized configuration is needed at the enterprise level based on information technology with various software testing tools. The security improvement impact is needed for risk management assessment and analysis with historical guidance and modern technological solution.

IV. RESULTS AND DISCUSSION

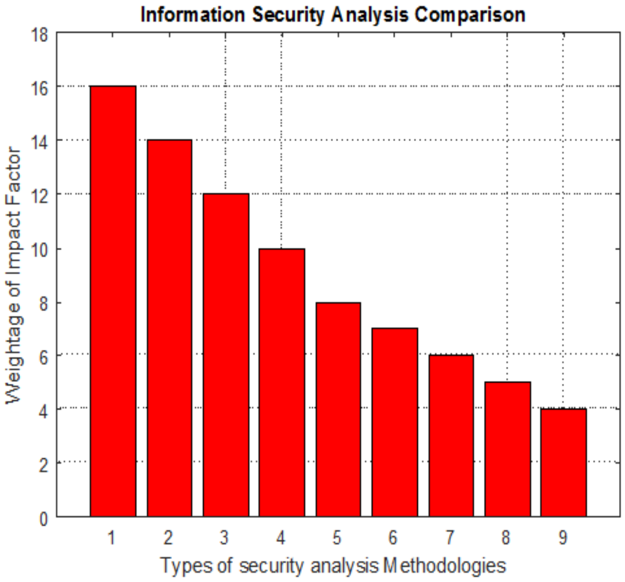

Figure 5: Comparison bar chart of information security analysis methodologies

The figure 5 shows that the comparison bar chart of information security analysis methodologies based on weight of impact factor. In the bar graph, OCTAVE Allegro have high impact factor than other methodologies based on its efficiency and its performance. From the figure 7, it is justified that the OCTAVE allegro is the best methodology for information security risk analysis methodology. In the bar graph the methodologies such as OCTAVE S, OCTAVE, CORAS, ISRM, IS, Risk Watch, COBRA, FRAP are plotted with respect to impact factor respectively.

Table 2: Comparison between risk analysis methodologies

CRITERIA	OCTAVE ALLEGRO	OCTAVE - S	OCTAVE	CORAS
Methods / Tools	Methods / Tools	Methods / Tools	Methods / Tools	Tools
Methods or Tool name	OCTAVE Allegro Ver 1.0	OCTAVE - S Ver 0.9 OCTAVE-S Ver 1.0	OCTAVE Framework, Ver 1.0 OCTAVE Framework, Ver 2.0	Coras editor Ver 1.1
Vendor name	Carnige Mellon University, SEI (Software Engineering Institute)	Carnige Mellon University, SEI (Software Engineering Institute)	Carnige Mellon University, SEI (Software Engineering Institute)	European Commission
Country of Origin	USA	USA	USA	Intracom (Greece), Solinet (Germany), Telenor (Norway)
Date of first Release	Jun 2007	Sep 2003	Sep 1999	Jan 2001
Official Website	http://www.cert.org/ octave allegro /owig.html	http://www.cert.org/ octaves/owig.html	http://www.cert.org/ octave/owig.html	http://www.peltierassiociates.com/frap.htm
Language	English	English	English	English
Price	Free	Free	Free	Free
Complaints to IT standard	ISO 3000, ISO / IEC	ISO 3000, ISO / IEC	ISO 3000 ISO / IEC	ISO 31000, ISO / IEC 17799, AS/NZS 4360
Skill needed	Standard	Standard	Standard	Standard
Tool supporting the method	Commercial tool Licensed tool seed threat identification, No needed of specialized knowledge and resources	Commercial tool, Licensed materials, Trainings (Sector with free availability: Educational support, awareness training)	Commercial tool, Licensed materials, Trainings (Sector with free availability: Educational support, awareness training)	An XML markup for exchange of risk assessment data A UML based specification language targeting security risk assessment
Availability	Original version	Train version, Original version with serial number	Train version, Original version with serial number	Train version, Original version with serial number

Table 3: Comparison between risk analysis methodologies

CRITERIA	ISRAM	IS Business	Risk Watch	FRAP	COBRA
Methods / Tools	Methods / Tools	Methods / Tools	Tools	Tool kit	Tool kit
Vendor Name	National Research Institute of Electronics and Cryptology, and the Gebze Institute of Technology	Korea Advanced Institute of Science and Technology	Risk Watch	The walk solution limited	C&A Systems Security

Methods or Tool name	ISRAM or ISRM	IS risk analysis based on business model	Risk Watch for information system, ISO 17799	FRAP risk management, E-business environment	The SRM COBRA tool
Country of Origin	Turkey	Seoul, Korea	USA	USA	United Kingdom
Date of first Release	Dec 2003	2002	2012	2000	May 2006
Language	English	English	English	English	English
Price	Free	Free	$15000, Free for education	$25,000	$1995
Complaints to IT standard	NIST SP 800-30, ISO/IEC 17799, ISO/IEC 13335	ISO 3000	ISO 3000	ISO 17799	ISO 17799
Skill needed	Standard	Standard	Standard	Need online help	Need online help
Tool supporting the method	Key risk management tool	Risk management tool	Management tool with features	FRAP method	COBRA risk management tool
Availability	Open	License	Open	License	License

V. CONCLUSION

Various methodologies are present in the healthcare sector for information security risk analysis with different task management. The nine methodologies are analyzed based on various problems including risk threats, economical requirement and development, human resources, vulnerabilities of risk occurrence. The OCTAVE family has the good impact fact than other methodologies. Based on the results, the OCTAVE Allegro methodology is superior to other methodologies in performance and efficiency for information security risk analysis.

REFERENCES

1. Armaghan Behnia, Rafhana Abd Rashid, Junaid Ahsenali Chaudhry, “A Survey of Information Security Risk Analysis Methods”, Smart Computing Review, vol. 2, no. 1, February 2012.
2. Richard A. Caralli, James F. Stevens, Lisa R. Young, William R. Wilson, “Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process”, Software Engineering Institute, May 2007
3. W.G. Bornman L, Labuschagne, “A COMPARATIVE FRAMEWORK FOR EVALUATING INFORMATION SECURITY RISK MANAGEMENT METHODS”, Standard Bank Academy for Information Technology, Rand Afrikaans University.
4. Ajit Appari and M. Eric Johnson, “Information security and privacy in healthcare: current state of research”, Int. J. Internet and Enterprise Management, Vol. 6, No. 4, 2010.
5. ANITA VORSTER AND LES LABUSCHAGNE, “A Framework for Comparing Different Information Security Risk Analysis Methodologies”, Proceedings of SAICSIT 2005.
6. John Shortreed, John Hicks, Lorraine Craig, “Basic Frameworks for Risk Management”, The Ontario Ministry of the Environment,2003.
7. Wayne L. Brannan, CPHRM, CBCP, ARM, Director, University Risk Management, “A Model for Enterprise Risk Management Within a Healthcare Organization”, The Medical University of South Carolina Charleston, South Carolina,2006.
8. Christopher J. Alberts Sandra G. Behrens William R. Wilson, “Managing Information Privacy & Security in Healthcare”, Health Information Risk Assessment and Management, 2007.
9. Johan Karlsson, “Information Structures and Workflows in Health Care Informatics”, Department of Computing Science Umea University,2010.
10. Bryan Cline, “A Security and Compliance Risk Management Framework for Health Care”,2009.
11. “HOW TO MANAGE WORK HEALTH AND SAFETY RISKS”, Government of South Australia code of practice, 2019.
12. Stefan Fenz, Andreas Ekelhart, “Information Security Risk Management: In Which Security Solutions Is It Worth Investing”, Communications of the Association for Information Systems,2011.
13. Arben Mullai, “Risk Management System – Risk Assessment Frameworks and Techniques”, Project partly financed by the European Union (European Regional Development Fund) within the BSR INTERREG III B programme,2006.
14. “A structured approach to Enterprise Risk management (ERM) and the requirement of ISO 31000”, AIRMIC, Alarm, IRM: 2010
15. Anand Singh, “Improving Information Security Risk Management”, THE FACULTY OF THE GRADUATE SCHOOL OF THE UNIVERSITY OF MINNESOTA, December 2009.

AUTHORS PROFILE

Amarendar Rao Thangeda, PhD in Computer science student of University of South Africa and Completed Master of Science in Computer Science and MTech in Computer Science. Having 21 years of teaching and administration experience.

Prof. Alfred Coleman, Associate Professor in School of Computing, College of Science and Engineering and Technology, University of South Africa and Completed PhD in Information Systems and MTech in Business Information Systems. More than 20 years of teaching and research experience.